Keith R. Nachbar
Bar No. 6-2808
Keith R. Nachbar, P.C.
703 N. Lincoln St.
Casper, Wyoming 82601
Telephone: (307) 473-8977
Fax: (307) 473-8989
keith@nachbarlaw.com

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF WYOMING

UNITED STATES OF AMERICA,	)	
	)	Criminal No. 23-CR-95-SWS
Plaintiff,	)	
	)	
v.	)	
	)	
PETER SZANTO,	)	
	)	
Defendant.	)	

MOTION TO SUPPRESS DATA OBTAINED FROM DEFENDANT'S INTERNET ACCOUNTS

COMES NOW Defendant Peter Szanto, by and through his attorney, Keith R. Nachbar of Keith R. Nachbar, P.C., and moves this Court for an order suppressing all evidence from the contents of Defendant's Internet accounts from Google, and T-Mobile, as a fruit of its unlawful seizure of these materials in violation of the Fourth Amendment.

INTRODUCTION

Defendant believes his private messages in his personal Internet account were seized at the government's direction under the claimed authority of a federal statute, 18 U.S.C. § 2703(f) (hereinafter, "the preservation statute").[1] The preservation statute provides that, "upon the request of a governmental entity," Internet providers "shall . . . retain" files in a user's account "for a period of 90 days," renewable for another 90 days. *Id.*

Defendant believes that the government ordered copies to be made of the contents of his Internet account, and to have those contents held for the government. It appears that Google and T-Mobile, acting as the government's agents, seized Defendant's private contents and held them on the government's behalf for an unknown amount of time. Defendant's counsel has requested to inspect the preservation letters in order to obtain accurate timelines however, the government has refused to allow Defendant to review the preservation letters sent to Google and T-Mobile.

This government-directed, suspicionless seizure of Defendant's personal messages cannot be reconciled with the Fourth Amendment.

[1]The Defendant is forced to assume (but does not know) that preservation letters preceded the seizure of Defendant's electronic data. Defendant requested copies of any preservation letters issued pursuant to the preservation statute and was advised by the United States that the letters would not be provided to Defendant.

Instead of preservation occurring "pending the issuance of a court order," 18 U.S.C. § 2703(f)(1), as the Fourth Amendment and the plain text of the statute require, the government appears to have used the preservation statute to gain control of Defendant's account just in case probable cause eventually developed. The government appears to have ordered the seizure of the accounts without probable cause or even reasonable suspicion. Indeed, the government did obtain an order pursuant to 18 U.S.C. § 2703(d), however, when asked for the initial preservation letters, the government would not provide them. This means that the Defendant has no idea the amount of time the government was constructively in possession of his records. 18 U.S.C. § 2703(b)(1)(A)(B) provides that a subscriber must be given notice unless the government obtains an actual search warrant for the data. 18 U.S.C. § 2703 (b)(1)(B)(ii) provides that the government may give delayed notice pursuant to section 2705 for certain purposes. Section 2705 provides that the government may delay notice to subscriber for certain purposes but only for a period not to exceed 90 days. Extensions may be given for an additional 90 days upon application by the government. Because the government has declined to turn over the preservation letters issued to Google and T-Mobile, the Defendant is unaware how long the government had constructively seized his data and is therefore

unsure if the government even properly complied with the notification requirement under the statute.

The Fourth Amendment protects the private e-mails and private messages in a password-protected online account. A government-directed copying and setting aside of a person's private account is a Fourth Amendment seizure. Such a warrantless seizure is permitted under the Fourth Amendment only in very limited circumstances, generally based on probable cause and permitted only for a brief period of time. Because the warrantless seizure in this case without any justification and for an extended period, the fruits of that seizure—the contents of the preserved account—must be suppressed.

In addition, beyond the improper seizure by the "preservation" mechanism of 18 U.S.C. § 2703(f)(1) for an unknown period of time, the government also failed to provide specific and articulable facts to support the issuance of an order for production of the internet materials under 18 U.S.C. § 2703(d), and failed to provide *any* facts in a sworn statement to support the issuance of an order under that section.

STATUTORY AND FACTUAL BACKGROUND

The Stored Communications Act, 18 U.S.C. §§ 2701-11, is a federal statute that regulates government access to the private records of Internet users. Internet providers such as Google and T-Mobile hold

their users' records on their computer network servers. When criminal investigators seek copies of records from the accounts of criminal suspects, investigators obtain the records directly from the Internet providers. The Stored Communications Act establishes the responsibilities and duties of both the government and Internet providers when the government seeks user information. *See generally* 2 Wayne LaFave, et al., Criminal Procedure § 4.8 (4th ed. 2015) (presenting overview of the statute).

This case involves the Stored Communications Act's preservation statute found at 18 U.S.C. § 2703(f). The statute provides:

> (f) Requirement To Preserve Evidence.
>
> (1) In general. — A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention. — Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The preservation statute was enacted to ensure government access to user records that might otherwise be deleted before the government obtained legal process. Because obtaining legal process can be time-consuming, the preservation statute "permits the government

to direct providers to 'freeze" stored records and communications" of suspects pending the issuance of a warrant or other court order. *U.S. Dep't of Just., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 139* (2009).

The key question is when the preservation statute can be used. In practice, it appears that the government and major Internet providers interpret 18 U.S.C. § 2703(f) to permit unlimited preservation of Internet accounts. The statute appears to allow any government agent, at any time, to order any provider to make and set aside a copy of every file, of any Internet account, without any suspicion whatsoever. The government calls this process "preservation." Acting on the government's instruction, and as the government's agents, Internet providers make complete copies of target accounts and save them exclusively for later government use.

This process is largely secret. When a government agent makes a § 2703(f) request, providers will copy and preserve the account contents. In the ordinary case, this process is hidden from users. Internet providers do not tell their customers that preservation occurred and the government ordinarily does not disclose preservation.

In this case, the Defendant is unaware whether preservation occurred. The Defendant can reasonably assume that the government

submitted a § 2703(f) request to Google and T-Mobile directing the preservation of Defendant's accounts, email addresses, and any other data desired by the government because typically preservation occurs before any warrant or order under § 2703(d) is ordered. In response to that request, Google and T-Mobile would have made a copy of Defendant's account at the time preservation was requested. Google and T-Mobile then would have set aside the copy and held it specifically for the government's use. Defendant is operating under the reasonable assumption that preservation occurred because when Defendant's counsel asked for any preservation letters, the government responded that it would not turn over any preservation letters. In addition, the common practice is for preservation to occur before a warrant or order is issued.

At some point in time after the preservation date, the government obtained an order under 18 U.S.C. § 2703(d) to justify the account's seizure and subsequent search. When the government submitted the order to Google and T-Mobile, the providers then complied with the order by sending the government the copy of the preserved account that had been created. Defendant now seeks the suppression of the preserved and produced account contents as the product of an unlawful seizure.

LEGAL ARGUMENT

The warrantless preservation of Defendant's Internet account violated his Fourth Amendment rights. The preservation was government action because it required Google and T-Mobile to act on the government's behalf. Preservation triggered a Fourth Amendment seizure because it eliminated Mr. Szanto's exclusive control of his account. It was an unreasonable seizure because it was not based on probable cause, reasonable grounds, reasonable suspicion, or even articulable facts, and there is no evidence that it was followed promptly by a warrant or an order. The contents of the account must be suppressed because they are fruits of the unconstitutional preservation, and the good-faith exception does not apply. The analysis below addresses each point in turn.

A. The Preservation of Defendant's Account Was Fourth Amendment State Action.

Google's and T-Mobile's acts of preserving Mr. Szanto's account pursuant to 18 U.S.C. § 2703(f) was government-directed action regulated by the Fourth Amendment. The Fourth Amendment applies to acts of private individuals acting as "instrument[s] or agent[s]" of the Government. *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971). A private party acts as a government agent when the government "compelled a private party to perform a search" or the private party

otherwise acted pursuant to the "encouragement, endorsement, and participation" of the government. *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614 (1989).

That test is satisfied here. Section 2703(f) states that "upon the request of a governmental entity," the provider "*shall take all necessary steps* to preserve records and other evidence" in its possession, and that the records "*shall be retained* for a period of 90 days, which *shall be extended* for an additional 90-day period upon a renewed request by the governmental entity." 18 U.S.C. § 2703(f) (emphasis added). By triggering the preservation statute, the government directed what Google and T-Mobile must do. In response, Google and T-Mobile fulfilled the government's wishes on the government's behalf. This mandate satisfies the test for state action. *See Skinner*, 489 U.S. at 613 (noting that "compell[ing] a private party to perform a search" makes that private party a Fourth Amendment state actor).

The preservation in this case is Fourth Amendment government action even if compliance with § 2703(f) is considered voluntary instead of a mandatory obligation. In *Commonwealth v. Gumkowski*, 167 N.E.3d 803 (Mass. 2021), a state trooper asked the cellular and Internet service provider Sprint to voluntarily disclose a suspect's cell-site location records without a warrant. Sprint agreed. The Court ruled

that Sprint's voluntary disclosure constituted Fourth Amendment state action: When "law enforcement instigates the search by contacting the cell phone company to request information, there is State action. That Sprint could have refused to provide records in response to [the state trooper's] request does not change the fact that he instigated the search." *Id.* at 812.

United States v. Hardin, 539 F.3d 404 (6th Cir. 2008), confirms the point. In *Hardin*, an apartment manager entered an apartment at the request of the government to see if the defendant was present. The Sixth Circuit ruled that the apartment manager was a Fourth Amendment state actor. *Id.* at 407. This was true, the court ruled, "because the officers urged the apartment manager to investigate and enter the apartment, and the manager, independent of his interaction with the officers, had no reason or duty to enter the apartment." *Id.*

When Google and T-Mobile complied with the government's directive under the preservation statute, both the government and the providers believed that the provider's compliance with the government's "request" was mandatory. The statute imposes an obligation: It states what a provider "shall" do when it receives a preservation request. 18 U.S.C. § 2703(f). This is not merely "instigat[ing]" the provider's act under *Gumkowski* and *Hardin*, it is "compell[ing] a private party" to act

under *Skinner*. But whether the preservation is construed as ordering or merely instigating the act of preservation, it is state action under the Fourth Amendment.

B. Preservation of Mr. Szanto's Account was a Fourth Amendment Seizure.

A Fourth Amendment seizure occurs "when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The classic example of a seizure is physical taking away of property. Being "dispossessed" of your property by government action causes a seizure of it. *Soldal v. Cook County*, 506 U.S. 56, 61 (1992) (towing away a mobile home).

Preservation of Mr. Szanto's account caused a Fourth Amendment seizure because it dispossessed him of control over the account. Internet providers "execute preservation requests by making a copy of the full contents of the relevant account and storing it separately." Kerr, *Internet Content Preservation*, at 771. Although this process is labeled 'preservation,' in reality it is "a dynamic process of entry, copying, and storage." *Id.* at 782. As Internet providers have themselves explained, this is done by performing a "data pull" of the contents of the account that take a "snapshot" of the account contents. *Id.* (quoting public statements from Twitter and Apple). The copy is

then stored outside the user's control so the user cannot alter or delete any files. *Id.* at 784-85.

The government-directed act of creating a government copy of the account, and storing it away for later government access, caused a "meaningful interference" with Mr. Szanto's "possessory interests in that property" because it denied him control over his private information. *Jacobsen*, 466 U.S. at 113. "Possession" is defined as the "detention and control. . . of anything which may be the subject of property." Black's Law Dictionary 1047 (5th ed. 1979). Before preservation occurred, Mr. Szanto had control of his account contents. He could view his files, he could alter his files, and he could delete his files as he wished.

Preservation eliminated that control. Preservation ensured that a perfect copy of the account contents was generated and detained outside his control exclusively for the government's future use. This was done for the express purpose, and with the exact effect, that Mr. Szanto could no longer control the contents of his account. The preservation notice therefore triggered a seizure. *See United States v. Bach*, 310 F.3d 1063, 1067-68 (8th Cir. 2002) (analyzing the copying and review of stored Internet contents held by an Internet provider as a Fourth Amendment "seizure" and a "search" of the contents); *Vaughn v.*

Baldwin, 950 F.2d 331, 334 (6th Cir. 1991) (noting that, in the absence of consent, the government had "no right to . . . photocopy" a person's private documents); *United States v. Loera,* 333 F. Supp. 3d 172, 185 (E.D.N.Y. 2018) ("Most courts that have addressed duplication, including digital duplication, have analyzed it as a seizure."); Fed. R. Crim. Pro. 41(e)(2)(B) (equating the seizure of electronically stored information with the copying of the information)[2].

In the data context, of course, the government dispossesses a person of control without physically removing the data. However, that makes no legal difference. Copying private files triggers a seizure because the government gains control of the data. The government's gaining control and a user's losing exclusive control causes a seizure even though the user still has access to a prior copy of the data. *See United States v. Jefferson,* 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (holding that "recording . . . information by photograph or otherwise" is a seizure, "even if the document or disc is not itself seized," because

[2] The Second Circuit expressly held that copying a file is a seizure in a panel decision that was later vacated on rehearing en banc; the en banc court did not reach the question. *See United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the Government's retention of electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which was "a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), *vacated by United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc).

"the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself"). The government cannot simply take control of the contents of everyone's private Internet messages, just as long as the government does not (yet) look at the files, entirely at the government's whim. Preservation triggers copying of the account, and that copying is a Fourth Amendment seizure permitted only if it is constitutionally reasonable. *See id.*

It should be especially clear that preservation is a Fourth Amendment "seizure" given how Internet search warrants are executed under the Stored Communications Act as required by the Fourth Amendment. *See Warshak v. United States*, 631 F.3d 266, 274 (6th Cir. 2010) (holding that accessing private emails is a Fourth Amendment search that requires a warrant). When the government serves a warrant on a provider under § 2703(a), the provider will run off a copy of the account and send the copy to the government for its review. The provider conducts the initial "seizure," and the government conducts the subsequent "search." *Cf. Bach*, 310 F.3d at 1067-68[3]. Preservation

[3] A small number of trial courts have reasoned that copying account contents are not seizures in the special context of copying files stored outside the United States. *See, e.g., United States v. Gorshkov*, 2001 WL 1024026, at 3 (W.D. Wash. May 23, 2001) (copying from a server in Russia); *In re Search Warrant To Google, Inc.*, 2017 WL 2985391, at 11 (D.N.J.

under § 2703(f) is the "seizure" part of the Stored Communications Act's procedure for obtaining Internet account contents. Preservation does not cause a search to occur, because information is not yet revealed to the government. However, the transfer of control of account contents under § 2703(f) is a seizure independently of any subsequent search, and it must be independently justified as reasonable. *See Soldal,* 506 U.S. at 61 (explaining that seizures must be justified under the Fourth Amendment independently of any searches).

C. The Government Cannot Satisfy Its Burden of Establishing that the Warrantless Seizure of the Account was Reasonable.

"If the defendant meets his burden of establishing a warrantless seizure, the burden then shifts. The Government must establish the warrantless seizure was reasonable." *United States v. Shrum*, 908 F.3d 1219, 1229 (10th Cir. 2018). Here the government cannot meet that burden. The contents of Mr. Szanto's Internet account were seized on an unknown date because the government has refused to provide that answer to the Defendant. Those contents were held without a warrant or order until an order was issued to permit the disclosure of the

---

2017) (copying accounts from servers outside the United States as part of the execution of a cloud warrant). This case does not raise the unique international concerns that underly those decisions.

account contents to the government. This government-directed suspicionless seizure, occurring for an undisclosed amount of time, cannot be upheld as reasonable under the Fourth Amendment.

D. The Government's Application for a 2703(d) Order Was Not Based On Sworn Specific and Articulable Facts.

Beyond the initial constructive seizure by the preservation mechanism, the government then actually obtained the Defendant's internet file data from Google and T-Mobile.[4] The statute upon which the government relied in seizing the Defendant's internet data was 18 U.S.C. § 2703(d), which states:

> "A court order for disclosure under subsection (b) or (c) may be issued by any court that is a **court of competent jurisdiction** and shall issue only if the **governmental entity** offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

The "specific and articulable facts" standard in § 2703(d) parallels the standard established in the Supreme Court's decision in *Terry v. Ohio. United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008). In justifying a particular intrusion, the police must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion. *Terry*

[4]Counsel is seeking permission to file copies of the applications and orders under seal.

v. Ohio, 392 U.S. 1, 21, 88 S. Ct. 1868, 1880, 20 L. Ed. 2d 889 (1968). It is imperative that the facts be judged against an objective standard: would the facts available to the officer at the moment of the seizure or the search 'warrant a man of reasonable caution in the belief' that the action taken was appropriate? *Id.* Anything less would invite intrusions upon constitutionally guaranteed rights based on nothing more substantial than inarticulate hunches. *Id.*

Here, the application is based on inarticulate hunches and possibilities rather than an objective standard because the creation of a corporation and the mere filing of a bankruptcy—both perfectly legal activities in themselves—would not 'warrant a man of reasonable caution' that illegal activity was afoot and that the seizure was appropriate. Mere hunches, beliefs, possibilities, and unsworn allegations are insufficient to grant an order to seize and search one's digital information, are constitutionally offensive, and intrude upon the Fourth Amendment. Conclusory statements do not satisfy the requirements of section 2703(d) . . . Nor does it allow for government fishing expeditions. *In re Applications of the United States of Am. For an Ord. Pursuant to 18 U.S.C. § 2703(d),* 206 F. Supp. 3d 454, 455 (D.D.C. 2016).

Here, the government's fact section of its request for a § 2703(d) order is hardly based on specific and articulable facts. The facts section states mere conclusory statements of the government's beliefs about the case, the mere possibilities of crimes, and its assertions about a "possible" case theory without a sworn affidavit or any other firsthand basis for those facts. Much of the information is obviously secondhand, and no basis or foundation is laid for any of the statements. The fact that a corporation was created and a bankruptcy was filed is woefully insufficient to request an order to seize a person's digital information. While the government has its "beliefs" and "possibilities" listed on its application as to why the corporation was created and why the bankruptcy was filed, "beliefs" and "possibilities" are nothing more than mere speculation and are not enough to meet the specific and articulable fact standard set out in the statute and in case law.

In the case of *In re Applications of the United States of Am. for an Ord. Pursuant to 18 U.S.C. § 2703(d),* 206 F. Supp. 3d 454, 455 (D.D.C. 2016), the court twice denied the government's application for a § 2703(d) order because the government gave no basis for the beliefs asserted in its request. The same problem exists here. The government asserts that a corporation was created "As part of a *possible* scheme" and asserts a bankruptcy was filed based on a belief that it was filed to

"continue his scheme" but then offers no basis for those beliefs. Likewise, the government admits in its unsworn application that it does not know if Ms. Jabotinsky, the person who created the corporation, exists. This demonstrates that the government did not even have readily obtainable specific facts to support its suspicions or theories.

It is also important to notice that the applications are not sworn or provided under any oath or affirmation. They are unsworn, based on secondhand information, and lack foundational footing. In the context of a search warrant, the Fourth Amendment requires that the judicial officer issuing a search warrant be supplied sufficient information, under oath or affirmation, which would support an independent judgment that probable cause exists for the warrant's issuance. *U. S. ex rel. Gaugler v. Brierley*, 477 F.2d 516, 522 (3d Cir. 1973). The 18 U.S.C. § 2703 statute itself does not specify whether the facts must be provided under oath or affirmation, but generally, statements must be made under oath to be considered evidence. 98 C.J.S. Witnesses § 445. It is difficult to conceive of a court in the United States properly issuing an order as invasive as a § 2703(d) order in the absence of a scintilla of actual *evidence*. *See In re Applications for Search Warrants for Info. Associated with Target Email Address*, No. 12-MJ-8119-DJW,

2012 WL 4383917, at 4 (D. Kan. Sept. 21, 2012)("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.") Even more troubling is the breadth of the orders based on the unsworn applications. They order production of parts of *all* communications for a period of months, without any filter or selection criteria at all. Under Tenth Circuit standards, they were impermissibly overbroad. *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005)(Holding that officers must describe with particularity the *objects of their search* and that Magistrates should, where appropriate, require officers to specify in a warrant which type of files are sought.)

The § 2703(d) applications and orders were improper. They were nothing more than unsworn suspicions of counsel for the government, based on second hand information, and lacking specific and articulable facts providing a reasonable suspicion of criminal activity. The things sought to be "investigated" are ordinarily legal activities. The orders issued by the magistrate judge were overly broad and did not properly describe the things sought.

E. The Entire Contents of Mr. Szanto's Accounts and Evidence Obtained from that Data Must be Suppressed as Fruit of the Poisonous Tree.

Defendant believes that the preserved copy of his Internet account was obtained by the government when it served an order on Google and T-Mobile. Because the government had access to that preserved copy as a result of its prior constitutional violation, and the subsequent improper § 2703(d) order, and the later search warrants were based on the preserved and obtained Internet data, the entire contents of Defendant's accounts must be suppressed as fruits of the poisonous tree under *Wong Sun v. United States*, 371 U.S. 471 (1963).

Suppression is appropriate when it "results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 141 (2009). That is the case here.

The good-faith exception of *Illinois v. Krull*, 480 U.S. 340 (1987), poses no barrier to suppression. *Krull* held that the exclusionary rule does not apply "when officers act in objectively reasonable reliance upon a statute authorizing warrantless administrative searches, but where the statute is ultimately found to violate the Fourth Amendment." *Id.* at 342. Officers are entitled to rely on legislative

judgments that searches are constitutional, *Krull* reasoned, at least when those legislative judgments are reasonable. *See id.* at 349-50.

Krull does not apply because the mistake here belongs to law enforcement instead of Congress. When Congress enacted 18 U.S.C. § 2703(f), it did not make any legislative judgments about what law enforcement seizures are permitted or when they are constitutional. The preservation statute is not directed to governments at all. The Fourth Amendment governs when a preservation request can be made, and the preservation statute does not say otherwise. The preservation statute merely specifies what Internet providers such as Google and T-Mobile must do when a government preservation request is made. "[U]pon the request of a governmental entity," the statute says, "[a] provider . . . shall take all necessary steps to preserve records and other evidence in its possession" 18 U.S.C. § 2703(f)(1).

It may be that investigators erroneously believed that § 2703(f) authorizes unlimited preservation. But, if so, that is a law enforcement mistake that falls outside *Krull*. Because there is no legislative error to defer to, the government cannot rely on *Krull* to avoid suppression. *See United States v. Wallace,* 885 F.3d 806, 811 n.3 (5th Cir. 2018) (noting, in a Fourth Amendment challenge brought to surveillance claimed to be authorized by the Stored Communications Act, that "[t]he

holding of *Krull* does not extend to scenarios in which an officer erroneously, but in good faith, believes he is acting within the scope of a statute").

Put another way, *Krull* only applies when a legislature enacts an unconstitutional law that law enforcement reasonably followed. Here, however, Congress enacted a perfectly constitutional law. Law enforcement's unconstitutional application of the preservation statute is law enforcement's fault, not the fault of Congress. The exclusionary rule should apply.

CONCLUSION

For the foregoing reasons, the Defendant respectfully requests that this Court suppress all evidence obtained as a result of the unlawful seizure of Defendant's account.

WHEREFORE, Mr. Szanto respectfully requests this Court:

(1) Find that Mr. Szanto's Fourth Amendment rights were violated;

(2) Suppress from introduction at his trial any information obtained as a result of data retention and production from Google and T-Mobile, as well as evidence obtained as a result of that data; and

(3) For such other and further relief as the Court deems just and equitable under the premises.

RESPECTFULLY SUBMITTED this 9th day of February 2024.

Peter Szanto, Defendant

By: /s/
Keith R. Nachbar
Bar No. 6-28-08
Keith R. Nachbar, P.C.
703 N. Lincoln St
Casper, Wyoming 82601
(307) 473-8977
keith@nachbarlaw.com

ATTORNEY FOR DEFENDANT